Patent Ordering

help

Enter Patent Type and Number: optional reference note

GO

Add patent to cart automatically. If you uncheck this box then you must *click on* Publication number and view abstract to Add to Cart.

1 Patent(s) in Cart

Patent Abstract

Add to cart

GER 2002-01-10 10030996 **Appliance and procedures to the control of business courses, especially at a vehicle,**

INVENTOR(S)- Wagner, Horst 70469 Stuttgart DE
INVENTOR(S)- Graf, Jens 97469 Gochsheim DE
INVENTOR(S)- Eberlein, Edwin 70197 Stuttgart DE

APPLICANT(S)- Robert Bosch GmbH 70469 Stuttgart DE

PATENT NUMBER- 10030996/DE-A1
PATENT APPLICATION NUMBER- 10030996
DATE FILED- 2000-06-30
DOCUMENT TYPE- A1, DOCUMENT LAID OPEN (FIRST PUBLICATION)
PUBLICATION DATE- 2002-01-10
INTERNATIONAL PATENT CLASS- G05B00902; G05B00902
PATENT APPLICATION PRIORITY- 10030996, A
PRIORITY COUNTRY CODE- DE, Germany, Ged. Rep. of
PRIORITY DATE- 2000-06-30
FILING LANGUAGE- German
LANGUAGE- German NDN- 203-0492-4256-3

Procedures and appliance about the control of business courses, especially at a vehicle, with what a function unit (101) with a bus system (105) stands in connection, with what the function unit is overseen the bus system und/oder by a supervision unit (102) and separates the connection (108, 104) the function unit with the bus system the

supervision unit in a security case through access, with what the access of the supervision unit is so konfigurierbar through the function unit, that the access path (110) of the supervision unit can be interrupted by a configuration means (103).

EXEMPLARY CLAIMS- 1. Procedure for the control of Betriebsablufen, in particular with a vehicle, whereby a functional unit with a bus system is located in connection, whereby the functional unit and/or the bus system are berwachungseinheit berwacht by one and berwachungseinheit the connection of the functional unit with the bus system in a safety case by access separate, by the fact characterized that that is access berwachungseinheit by the functional unit configurable. 2. Procedure according to requirement 1, by the fact characterized that that is in such a manner configurable access that the functional unit with a configuration means, in particular, in connection stands for a storage area and writes into the configuration means at least one configuration value or from the configuration means lscht and that is mglich access berwachungseinheit only at written configuration value. 3. Procedure according to requirement 1, by the fact characterized that with a system that enthlt at least the functional unit and berwachungseinheit different modes of operation is differentiated and abhngig from the modes of operation that access is berwachungseinheit configured. 4. Procedure according to requirement 3, by the fact characterized that access abhngig by at least one of the following modes of operation one configures to that: System operation, system wake, system advance, systems programming, Systemprfung, system simulation and/or-application. 5. Procedure according to requirement 2 and 3, thereby are used is used marked that several configuration values, and for each mode of operation its own configuration value and/or per mode of operation different configuration values to be differentiated. 6. Device for the control of Betriebsablufen with the vehicle, with a functional unit, in particular a control unit, which exhibit a connection to a bus system, as well as one berwachungseinheit in particular, which berwacht the functional unit and/or the bus system, whereby the connection of

NO-DESCRIPTORS

Nerac, Inc. One Technology Drive . Tolland, CT
Phone (860) 872-7000 Fax (860) 875-1749

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 30 996 A 1**

(51) Int. Cl.[7]: G 05 B 9/02

(21) Aktenzeichen: 100 30 996.8
(22) Anmeldetag: 30. 6. 2000
(43) Offenlegungstag: 10. 1. 2002

DE 100 30 996 A 1

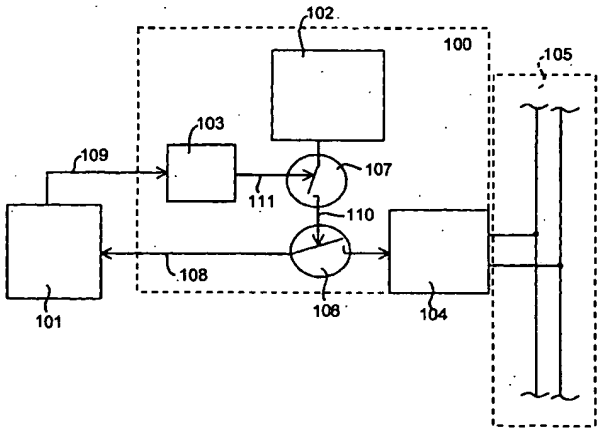
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Wagner, Horst, 70469 Stuttgart, DE; Graf, Jens, 97469 Gochsheim, DE; Eberlein, Edwin, 70197 Stuttgart, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Vorrichtung und Verfahren zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug

(57) Verfahren und Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug, wobei eine Funktionseinheit (101) mit einem Bussystem (105) in Verbindung steht, wobei die Funktionseinheit und/oder das Bussystem durch eine Überwachungseinheit (102) überwacht werden und die Überwachungseinheit die Verbindung (108, 104) der Funktionseinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff trennt, wobei der Zugriff der Überwachungseinheit durch die Funktionseinheit derart konfigurierbar ist, dass durch ein Konfigurationsmittel (103) der Zugriffpfad (110) der Überwachungseinheit unterbrochen werden kann.



DE 100 30 996 A 1

Beschreibung

Stand der Technik

[0001] Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug. Gemäß den Oberbegriffen der unabhängigen Ansprüche steht dabei eine Funktionseinheit mit einem Bussystem in Verbindung, wobei die Funktionseinheit und/oder das Bussystem durch eine Überwachungseinheit überwacht werden und die Überwachungseinheit die Verbindung der Funktionseinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff trennt.

[0002] Dazu ist aus der EP 0 983 905 A2 eine Schaltungsanordnung zur Abkopplung einer elektronischen Einrichtung von einer Datenleitung in einem Kraftfahrzeug bekannt. Über die Datenleitung tauschen die elektronische Einrichtung und wenigstens ein weiteres elektrisches System in ihrem Betrieb Informationen aus. Bei der Schaltungsanordnung, bei welcher trotz Ausfall einer an die Datenleitung angeschlossenen elektronischen Einrichtung der Fahrzeugbetrieb aufrechterhalten werden kann, ist die elektronische Einrichtung mit einer Fehlererkennungseinrichtung verbunden. Bei Feststellung eines Fehlers der elektronischen Einrichtung durch die Fehlererkennungseinrichtung wird die elektronische Einrichtung von der Datenleitung durch die Schaltungsanordnung abgekoppelt, wobei die Betriebsfähigkeit des elektrischen Systems aufrechterhalten bleibt.

[0003] Daneben zeigt der VDI-Bericht Nr. 687, 1988 "Antriebsschlupfregelung – Realisierung bei Audi", Seite 219 bis 222, eine Elektronik mit zwei Mikroprozessoren, welche sich gegenseitig überwachen und von denen einer eine Endstufe ansteuert. Dabei kann jeder Prozessor im Fehlerfall eine Sicherheitsschaltung aktivieren, welche dann die Rücksetzleitungen der Mikroprozessoren aktiviert und für definierte Softwareabarbeitung sorgt. Ein eventuell auftretender Defekt in der Endstufe kann nach Rückmeldung an den Prozessor durch Deaktivierung der Endstufenansteuerung abgefangen werden oder, sollte dies nicht greifen, durch Betätigung des Hauptrelais in der Sicherheitsschaltung durch jeden der beiden Prozessoren.

[0004] Bei den aus dem Stand der Technik bekannten Systemen ist eine Wiederankopplung der elektronischen Einrichtung an das elektrische System ebenso wie eine Verhinderung der Abtrennung in bestimmten Situationen nicht vorgesehen. Insbesondere bei Fehlerheilung wäre eine leicht handhabbare Wiederankopplung der elektronischen Einrichtung an das elektrische System oder die Verhinderung einer sofortigen Abtrennung wünschenswert.

[0005] Zum anderen kann ein Sicherheitsfall, welcher eine Abtrennung der elektronischen Einheit vom elektrischen System durch eine Sicherheitsschaltung nach sich zieht in bestimmten Betriebsarten bzw. Betriebszuständen nicht problematisch oder sogar gewünscht sein. Die zwingende Abtrennung im Stand der Technik wäre dann eher ungünstig. Durch einfache Wiederankopplung oder Verhinderung der Abtrennung für diese Betriebszustände könnte diese Situation leicht gehandhabt werden. Der Sicherheitsfall würde dann entgegen dem Stand der Technik für diese Zustände nicht zu einer Abtrennung führen, da die Ursachen für den Sicherheitsfall in diesen Zuständen nicht sicherheitskritisch sind.

[0006] Deshalb soll durch die Erfindung ein Verfahren und eine Vorrichtung geschaffen werden, welche die Funktionalität bei einer Steuerung von Betriebsabläufen im Hinblick auf die Abtrennung im Sicherheitsfall gemäß obiger Ausführungen optimiert.

Vorteile der Erfindung

[0007] Dabei geht die Erfindung aus von einem Verfahren und einer Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug, wobei eine Funktionseinheit mit einem Bussystem in Verbindung steht und die Funktionseinheit und/oder das Bussystem durch eine Überwachungseinheit überwacht werden. Dabei trennt die Überwachungseinheit die Verbindung der Funktionseinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff. Dieser Zugriff der Überwachungseinheit soll dann vorteilhafter Weise durch die Funktionseinheit konfigurierbar sein. Dadurch kann in bestimmten Situationen eine Abtrennung der Funktionseinheit vom Bussystem verhindert werden. Ebenso kann dadurch die eventuell bereits in einer Situation oder einem Betriebszustand abgetrennte Funktionseinheit in einer anderen Situation oder einem anderen Betriebszustand wieder angekoppelt werden.

[0008] Dabei wird vorteilhafter Weise der Zugriff derart konfiguriert, dass die Funktionseinheit, welche mit einem Speicherbereich in Verbindung steht oder diesen enthält, in diesen Speicherbereich wenigstens einen Konfigurationswert schreibt oder aus diesem Speicherbereich löscht, wobei der Zugriff der Überwachungseinheit nur bei eingeschriebenem Konfigurationswert möglich ist.

[0009] Als weitere vorteilhafte Ausgestaltung kann vorgesehen sein, dass abhängig von unterschiedlichen Konfigurationswerten, welche überprüft werden, in unterschiedlichen Betriebsarten bzw. Betriebszuständen der Zugriff der Überwachungseinheit möglich ist oder gesperrt wird.

[0010] Dabei werden zweckmäßiger Weise verschiedene Betriebsarten bei einem System, welches wenigstens die Funktions- oder Steuereinheit und die Überwachungseinheit enthält unterschieden, wobei der Zugriff der Überwachungseinheit dann abhängig von den Betriebsarten konfiguriert wird.

[0011] Zweckmäßiger Weise werden dabei folgende Betriebsarten unterschieden und der Zugriff abhängig von wenigstens zwei dieser Betriebsarten konfiguriert: Systembetrieb, Systemnachlauf, Systemvorlauf, Systemprogrammierung, und Systemsimulation bzw. Systemapplikation.

[0012] In einer vorteilhaften Ausgestaltung des erfindungsgemäßen Gegenstandes ist die Überwachungseinheit, eine Verbindungseinheit zur Anbindung an ein Bussystem, insbesondere als Bustreiber, und ein Konfigurationsmittel, insbesondere als Speichermittel bzw. Speicherbereich oder Register, zur Konfiguration des Zugriffs der Überwachungseinheit, als eine räumlich integrierte Baugruppeneinheit zusammengefaßt bzw. als ein Schaltkreis als IC integriert.

[0013] Somit können vorteilhafter Weise im Sicherheitsfall im Systembetrieb keine potentiell falschen oder nicht gewünschten CAN-Werte versendet werden, wodurch eigensichere Einzelsysteme im Netzwerkverbund entstehen.

[0014] Daneben wird zweckmäßiger Weise gewährleistet, daß z. B. für die Steuergeräteprüfung oder -programmierung und gegebenenfalls im Nachlauf oder anderen Betriebsarten sich der Funktionsrechner bzw. die Funktionseinheit durch eine geeignete Prozedur freischalten kann. Dazu wird vorteilhafter Weise dann in einer Ausführungsform z. B. der Konfigurationswert durch den Funktionsrechner gelöscht wodurch dieser trotz ansprechendem Überwachungsmodul bz. Überwachungseinheit weiter CAN-Botschaften versenden kann. Weitere Vorteile und vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Ansprüche und der Beschreibung.

Zeichnung

[0015] Die Erfindung wird im weiteren anhand der in der Zeichnung dargestellten Figuren beschrieben.

[0016] In **Fig.** 1 ist schematisch eine erfindungsgemäße Vorrichtung mit Überwachungseinheit, Funktionseinheit, Verbindungseinheit und Speicherbereich dargestellt.

[0017] Ein entsprechendes erfindungsgemäßes Verfahren wird in **Fig.** 2 in Form eines Flußdiagramms dargestellt.

Beschreibung der Ausführungsbeispiele

[0018] In **Fig.** 1 ist eine Funktionseinheit **101** beispielsweise eine Steuereinheit zur Steuerung von Betriebsabläufen bei einem Fahrzeug dargestellt. Diese Funktionseinheit **101** ist über ein System von Datenleitungen, insbesondere ein Bussystem, mit weiteren Funktionseinheiten, insbesondere weiteren Steuereinheiten, Aktuatorik oder Sensorik, verbunden. Am Bussystem **105** sind weitere Funktionseinheiten als weitere Busteilnehmer angekoppelt, die aber im einzelnen nicht dargestellt sind. Die Summe der weiteren Funktionseinheiten mit den Datenleitungen könnte auch im Bussystem **105** zusammengefaßt werden.

[0019] Die Verbindung zum Bussystem **105** ist in **Fig.** 1 symbolisch als bidirektionale Verbindung **108** und eine Verbindungseinheit **104** dargestellt. Dabei stellt die Verbindungseinheit **104** beispielsweise eine Signalverstärkungseinrichtung, insbesondere eine Bustreiberschaltung z. B. einen CAN-Treiber für ein CAN-Bussystem dar. Die Funktionseinheit **101** bzw. das Bussystem **105** und/oder der Bustreiber **104** sind durch eine Überwachungseinheit **102** kontrollierbar. Beispielsweise anhand von Signalen des Bussystems **105** der Verbindungseinheit **104** oder der Funktionseinheit **101** erkennt die Überwachungseinheit **102** Fehlfunktionen, oder sonstige einen Sicherheitsfall hervorrufende Ursachen.

[0020] Ein solcher Sicherheitsfall kann bei Fehlern im System auftreten, aber auch z. B. im Systemnachlauf bei Parametereinstellungen oder beispielsweise bei Initialisierungsvorgängen im Systemvorlauf. Diese Initialisierungsvorgänge im Systemvorlauf können aber z. B. bei einer Programmierung, Simulation, Applikation oder Prüfung gewünscht sein. Ein Sicherheitsfall, z. B. ausgelöst im Systemvorlauf sollte dabei nicht die Abtrennung der Verbindung der Funktionseinheit mit dem Bussystem durch Zugriff der Überwachungsschaltung zur Folge haben. Ebenso sollten bestimmte Vorgänge bei der Systemprogrammierung, der Systemprüfung oder der Systemsimulation bzw. Systemapplikation, welche eigentlich im normalen Systembetrieb, z. B. dem Fahrbetrieb eines Fahrzeugs, einen Sicherheitsfall auslösen würden, aber in diesen Betriebsarten gewünscht sind keinen wirkenden Zugriff des Überwachungsmoduls zur Folge haben. Im Systembetrieb selbst, also z. B. im Fahrbetrieb wird aber das Versenden von Botschaften durch die Funktionseinheit in einem solchen Sicherheitsfall durch die Überwachungseinheit bzw. das Überwachungsmodul unterbunden.

[0021] Somit können im Sicherheitsfall im Systembetrieb keine potentiell falschen oder nicht gewünschten CAN-Werte versendet werden, wodurch eigensichere Einzelsysteme im Netzwerkverbund entstehen.

[0022] Daneben wird gewährleistet, daß z. B. für die Steuergeräteprüfung oder -programmierung und gegebenenfalls im Nachlauf oder anderen Betriebsarten sich der Funktionsrechner bzw. die Funktionseinheit durch eine geeignete Prozedur freischalten kann. Dazu wird dann in einer Ausführungsform z. B. der Konfigurationswert durch den Funktionsrechner gelöscht wodurch dieser trotz ansprechendem Überwachungsmodul weiter CAN-Botschaften versenden kann.

[0023] Dabei kann eine einzelne Überwachungseinheit ebenso vorgesehen sein, wie jeweils eine Überwachungseinheit für jede oder auch für mehrere Funktionseinheiten, wobei dann die in **Fig.** 1 dargestellte Anordnung prinzipiell bei jedem Busteilnehmer bzw. für eine Gruppe von Busteilnehmern eingesetzt würde.

[0024] Die Überwachungseinheit **102** steuert bzw. bedient ein erstes Zugriffselement **106** durch welches im Sicherheitsfall die Verbindung **108** unterbrochen werden kann. In einer weiteren Ausführungsform kann der Zugriff der Überwachungseinheit auch auf die Verbindungseinheit **104** direkt erfolgen, wobei dann in der Verbindungseinheit **104** selbst die Unterbrechung der Funktionseinheit **101** zum Bussystem **105** initiiert wird, beispielsweise durch ein Zugriffselement in der Verbindungseinheit **104**.

[0025] Neben dem ersten Zugriffselement **106** ist im Zugriffspfad **110** der Überwachungseinheit auf die Verbindung von Funktionseinheit **101** zu Bussystem **105** ein zweites Zugriffselement **107** vorgesehen. Dieses zweite Zugriffselement **107** wird über Zugriffspfad **111** durch ein Konfigurationsmittel **103** bedient. Das Konfigurationsmittel **103** selbst wird über Pfad **109** durch die Funktionseinheit **101** angesprochen.

[0026] In einem bevorzugten Ausführungsbeispiel ist das Konfigurationsmittel **103** lediglich als ein Speichermittel bzw. ein Speicherbereich ausgebildet, in welchen wenigstens ein Konfigurationswert eingeschrieben bzw. aus welchem dieser gelöscht wird. Das Einschreiben, bzw. Löschen des Konfigurationswertes im Speichermittel **103** führt die Funktionseinheit **101** über Pfad **109** durch. Abhängig von dem Konfigurationswert im Speichermittel **103** wird der Zugriff bzw. der Zugriffspfad **110** der Überwachungseinheit **102** konfiguriert. Im einfachsten Fall erfolgt die Konfiguration derart, dass ein eingeschriebener Konfigurationswert TDI (Transmit Disable) den Zugriff der Überwachungseinheit **102** auf die Verbindung von Funktionseinheit **101** und Bussystem **105** also Verbindungspfad **108** bzw. Verbindungseinheit **104** unterbindet. Dies kann einerseits dadurch geschehen, dass die Überwachungseinheit **102** vor jedem Zugriff den Speicherbereich bzw. das Speichermittel als Konfigurationsmittel **103** auf die Präsenz des Konfigurationswertes TDI untersucht und nur bei fehlendem Wert TDI einen Zugriff durchführt wird oder das ein eingeschriebener Konfigurationswert TDI von vornherein eine Blockierung des Zugriffs, also des Zugriffspfades **110** der Überwachungseinheit **102** zu Folge hat. Somit ist das zweite Zugriffselement **107** symbolisch zu verstehen. Dies kann einerseits ein tatsächliches Schaltmittel zum Öffnen und Schließen des Zugriffspfades sein, andererseits kann diese Funktion auch in Software in der Überwachungseinheit **102** oder im Zugriffspfad **110** oder auch im Konfigurationsmittel **103** realisiert sein.

[0027] Gleiches gilt im Prinzip auch für das erste Zugriffselement **106**, wobei aus Sicherheitsgründen eine Realisierung als Schaltmittel und damit eine galvanische Trennung der Funktionseinheit **101** vom Bussystem **105** bzw. der Verbindungseinheit **104** zweckmäßig ist.

[0028] In einer vorteilhaften Ausgestaltung des erfindungsgemäßen Gegenstandes ist die Überwachungseinheit **102**, die Verbindungseinheit **104**, insbesondere als Bustreiber, und das Konfigurationsmittel **103**, insbesondere als Speichermittel bzw. Speicherbereich oder Register als integrierte Baugruppeneinheit **100** zusammengefaßt bzw. als ein Schaltkreis als IC integriert.

[0029] Der Funktionsrechner bzw. die Funktionseinheit **101** kann den. Konfigurationswert TDI über eine beispiels-

weise serielle Datenverbindung **109** setzen und löschen. Ein beispielhafter Ablauf kanh dann wie folgt, insbesondere für ein Fahrzeug, dargelegt werden:

[0030] Beim Einschalten des Systems, welches wenigstens Funktionseinheit **101** und Überwachungseinheit **102** enthält, ist der Konfigurationswert TDI gelöscht. Die Funktionseinheit **101** kann ohne Bedienung der Überwachungseinheit **102** senden, d. h. der Zugriff der Überwachungseinheit ist gesperrt. Bevor der Betrieb, insbesondere bei einem Fahrzeug der Fahrbetrieb, aufgenommen wird, wird der Konfigurationswert TDI gesetzt. Somit ist für den Betriebsfall, insbesondere den Fahrbetrieb bei Fahrzeugen die Sicherheit insofern gewährleistet, als das ein Versenden von Busbotschaften, insbesondere CAN-Botschaften im Sicherheitsfall durch die Überwachungseinheit **102** unterbunden werden kann. Im Rahmen einer besonderen Betriebsart bzw. einem besonderen Betriebszustand beispielsweise dem Systemnachlauf, Systemvorlauf einer Systemprogrammierung, einer Systemprüfung oder Systemsimulation kann dann der Konfigurationswert TDI wieder gelöscht werden. Somit kann z. B. ohne Bedienung der Überwachungseinheit **102** eine Neu- bzw. Umprogrammierung des Steuergerätes, insbesondere der Funktionseinheit **101** oder auch einer anderen am Bus angekoppelten Steuereinheit durch die Funktionseinheit **101** via das Bussystem **105** erfolgen.

[0031] Dabei kann die Prozedur zum Setzen bzw. Löschen des Konfigurationswertes TDI zusätzlich abgesichert werden. Beispielsweise müssen zuerst andere Speicherbereiche bzw. Register geeignet beschrieben werden und/oder ein, insbesondere codierter, Schreibschutz aufgehoben werden.

[0032] Die Darstellung eines solchen erfindungsgemäßen Verfahrens ist im Rahmen des Flußdiagramms in **Fig. 2** dargestellt. Block **200** markiert dabei den Start, speziell das Einschalten des Systems. In Abfrage **201** wird überprüft, ob der Systembetrieb, insbesondere der Fahrbetrieb bei Fahrzeugen vorgesehen ist.

[0033] Diese Überprüfung kann mit tatsächlichen Betriebsgrößen wie Motordrehzahl, Geschwindigkeit oder anderen durchgeführt werden. Andererseits ist eine Überprüfung anhand spezieller Werte oder Systembetriebsgrößen möglich, die für bestimmte Betriebszustände wie den Fahrbetrieb vorhanden sind bzw. bestimmte Werte einnehmen und für andere Betriebszustände wie einen Programmierbetrieb fehlen oder andere Werte einnehmen. Dabei können auch ganze Softwareteile die für einzelne Betriebszustände geladen bzw. vorhanden sein müssen für andere Betriebszustände fehlen woraus ebenfalls speziell auf den Fahrbetrieb vorab geschlossen werden kann.

[0034] Wird in Abfrage **201** erkannt, dass ein Fahrbetrieb vorgesehen ist, gelangt man zu Block **202** wo die Funktionseinheit **201** den Konfigurationswert TDI im Konfigurationsmittel **103**, insbesondere im Speichermittel setzt. In der darauffolgenden Abfrage **203** wird nochmals überprüft, ob ein Fahrbetrieb vorliegt. Ist dies der Fall, gelangt man zu Abfrage **204** in welcher nun die Überwachungseinheit den Sicherheitsfall kontrolliert. Liegt kein Sicherheitsfall vor, gelangt man zu Block **205** wo die gewünschten Funktionen und Programme im Rahmen des Fahrbetriebs ausgeführt werden.

[0035] Von Block **205** gelangt man erneut zur Abfrage **203** und der Kontrolle ob bzw. ob weiter ein Fahrbetrieb vorliegt. Ist dies nicht der Fall, gelangt man zu Abfrage **207**, zu der ebenso von Abfrage **201** verzweigt wird wenn in dieser festgestellt wird, dass kein Fahrbetrieb vorgesehen ist.

[0036] In Abfrage **207** wird überprüft, ob ein anderer Betriebsfall vorliegt. In **Fig. 2** ist beispielhaft nur ein weiterer Betriebsfall aus Gründen der Übersichtlichkeit gewählt. Ebenso könnten weitere Betriebsarten bzw. Betriebsfälle nacheinander analog der dargestellten Form geprüft werden. Diese weiteren Betriebsfälle sind beispielsweise der Systemnachlauf oder Nachlaufbetrieb, der Systemvorlauf oder Vorlaufbetrieb, die Systemprogrammierung, Systemprüfung oder Systemsimulation bzw. -applikation.

[0037] Liegt also der weitere Betriebsfall in Abfrage **207** nicht vor, gelangt man zu Block **215**, in welchem der Konfigurationswert TDI durch die Funktionseinheit bzw. den Funktionsrechner **101** gelöscht wird und dann zum Verfahrensende in Block **216**. Liegt wenigstens ein weiterer Betriebsfall vor, gelangt man zu Block **212** und optional zu Block **208o**. In Block **212** wird der Konfigurationswert TDI durch den Funktionsrechner bzw. die Funktionseinheit gelöscht. Danach wird in Block **213** der weitere Betriebsfall auf den in Abfrage **207** geprüft wurde im Rahmen der dabei nötigen Funktionen und Programme durchgeführt.

[0038] In Abfrage **214** wird kontrolliert, ob der weitere Betriebsfall noch vorliegt, bzw. dieser weiterhin ausgeführt werden soll. Ist dies der Fall, gelangt man wieder zu Block **213** wo weitere Funktionen bzw. Programme des weiteren Betriebsfalls ausgeführt werden. Ist der weitere Betriebsfall beendet, bzw. abgeschlossen, gelangt man zu Block **216** dem Verfahrensende.

[0039] Durch den gelöschten Konfigurationswert TDI in Block **212** ist im weiteren **213**, **214** sichergestellt, dass die Überwachungseinheit **102** das erste Zugriffselement **106** mittels Zugriffspfad **110** nicht bedienen kann. Damit wird gewährleistet, dass beispielsweise für die Steuergeräteprüfung/-programmierung oder im Nachlauf also in einer der weiteren Betriebsarten die Funktionseinheit bzw. der Funktionsrechner sich durch eine geeignete Prozedur freischalten kann. Dazu löscht der Funktionsrechner **101** den Konfigurationswert TDI und kann dann trotz beispielsweise ansprechender Überwachungseinheit **102** noch Busbotschaften versenden.

[0040] Im Sicherheitsfall, beispielsweise erkannt durch Abfrage **204** bei gesetztem (Block **202**) Konfigurationswert TDI trennt nämlich die Überwachungseinheit **102** die Verbindung Funktionseinheit, bzw. Funktionsrechner **101** und Bussystem **105** bzw. Verbindungseinheit **104**. Dies wird bei Erkennung eines Sicherheitsfalls in Abfrage **204** in Block **206** durchgeführt. Ein weiterer Fahrbetrieb ist danach in der Regel dennoch möglich und wird in Abfrage **203** erneut abgefragt.

[0041] Optional eingefügt ist Block **208o**. Dieser Block kann zur Erhöhung der Sicherheit zusätzlich eingebracht werden. Darin gelangt man dann aus Abfrage **207** für den Fall das der weitere Betrieb vorliegt zur Abfrage **209o**. Darin wird nun überprüft, ob ein Sicherheitsfall bei Abfrage **204** vorliegt oder nicht. Liegt kein Sicherheitsfall vor, gelangt man wieder zu Block **212**.

[0042] Ist aber ein Sicherheitsfall aufgetreten, wird in Abfrage **210o** abgefragt, ob der Konfigurationswert TDI gesetzt werden soll oder nicht. Dies hat den Hintergrund, dass in einem zum Systembetrieb, insbesondere zum Fahrbetrieb, unterschiedlichen Betriebsart bzw. Betriebsfall ein erkannter Sicherheitsfall, wie oben ausgeführt nicht zwangsläufig die gleiche Bedeutung hat wie im Fahrbetrieb. Gerade in den genannten Betriebsfällen können Bedingungen bzw. Zustände die im Systembetrieb sofort zu einer Verbindungstrennung führen würden, durchaus gewünscht sein.

[0043] Stellt sich also heraus, dass zwar durch die Überwachungseinheit ein Sicherheitsfall erkannt wurde der Konfigurationswert TDI aber nicht gesetzt werden muß bzw. darf weil bezüglich der anderen Betriebsart die Zustandskombination gewünscht ist, gelangt man ebenfalls zu Block **212** worin der Konfigurationswert gelöscht wird sofern er gesetzt war. Stellt sich in Abfrage **210o** heraus, dass der Si-

cherheitsfall sehr wohl kritisch ist, beispielsweise aufgrund eines schwerwiegenden Defektes, welcher auch für die weitere Betriebsart problematisch ist so wird in Block **211**o der Konfigurationswert TDI gesetzt bzw. sofern dieser bereits gesetzt ist, nicht gelöscht und man gelangt zu Block **206**, worin erneut die Verbindung durch die Überwachungseinheit **102** getrennt wird.

[0044] Somit wird das Versenden von Bus-, insbesondere CAN-Botschaften im Sicherheitsfall durch die Überwachungseinheit **102** unterbunden. Diese Unterbindung ist durch die Funktionseinheit bzw. in Funktionsrechner **101** konfigurierbar, in dem dieser den Konfigurationswert TDI (Transmit Disable) setzt bzw. löscht.

[0045] In einer weiteren vorteilhaften Ausgestaltung ist eine feinere Differenzierung im Rahmen des Konfigurationswertes denkbar. Dabei ist nicht allein das Setzen oder Nichtsetzen des Konfigurationswertes von Bedeutung sondern es spielt eine Rolle, welcher Konfigurationswert gesetzt ist. So kann z. B. nach Betriebsarten unterschieden mit unterschiedlichen Konfigurationswerten je nach Betriebsart differenziert werden, ob die Funktionseinheit in die Lage versetzt wird, den Zugriff der Überwachungseinheit zu konfigurieren oder nicht. So gilt ein Konfigurationswert beispielsweise ausschließlich für die Systemprogrammierung. Ein Löschen dieses Konfigurationswertes läßt eine Systemprüfung trotz Sicherheitsfall aber nicht zu, dazu müßte ein anderer Konfigurationswert gelöscht werden bzw. der Konfigurationswert müßte ein anderer sein.

[0046] Bei Einsatz eines Fehlerzählers z. B. ist denkbar, dass ein Konfigurationswert TDI1 diesen sperrt, so dass dieser seinen Maximalwert, der den Sicherheitsfall repräsentiert nicht erreichen kann. Ein zweiter Konfigurationswert TDI2 überbrückt den Fehlerzähler und läßt den Zugriff des Überwachungsmodules trotz längst erreichtem Maximalwert nicht zu. Dies hat den Vorteil, dass bei Löschen von TDI2 sofort der Zugriff der Überwachungseinheit erfolgt wohingegen im ersten Fall bei TDI1 erst der Maximalwert des Zählers nach Löschen von TDI1 erreicht werden muß. Mehere Konfigurationswerte TDI1, TDI", ... können dann je Betriebsart oder für alle Betriebsarten gemeinsam eingesetzt werden.

[0047] Damit gewährleistet die Erfindung, dass im Sicherheitsfall keine potentiell falschen Bus- bzw. CAN-Werte gesendet werden können. Dies ist eine wichtige Eigenschaft für eigensichere Einzelsysteme in einem Netzverbund. Gleichzeitig kann aber eine Korrektur beispielsweise des aufgetretenen Fehlers erfolgen, weil beispielsweise eine Neuprogrammierung trotz ansprechende Überwachungseinheit offengehalten wird.

Patentansprüche

1. Verfahren zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug, wobei eine Funktionseinheit mit einem Bussystem in Verbindung steht, wobei die Funktionseinheit und/oder das Bussystem durch eine Überwachungseinheit überwacht werden und die Überwachungseinheit die Verbindung der Funktionseinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff trennt, **dadurch gekennzeichnet**, dass der Zugriff der Überwachungseinheit durch die Funktionseinheit konfigurierbar ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Zugriff derart konfigurierbar ist, dass die Funktionseinheit mit einem Konfigurationsmittel, insbesondere einem Speicherbereich, in Verbindung steht und in das Konfigurationsmittel wenigstens ein Konfigurationswert schreibt oder aus dem Konfigurationsmittel löscht und der Zugriff der Überwachungseinheit nur bei eingeschriebenem Konfigurationswert möglich ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass bei einem System das wenigstens die Funktionseinheit und die Überwachungseinheit enthält verschiedene Betriebsarten unterschieden werden und abhängig von den Betriebsarten der Zugriff der Überwachungseinheit konfiguriert wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass der Zugriff abhängig von wenigstens einer der folgenden Betriebsarten konfiguriert wird: Systembetrieb, Systemnachlauf, Systemvorlauf, Systemprogrammierung, Systemprüfung, Systemsimulation und/oder -applikation.

5. Verfahren nach Anspruch 2 und 3, dadurch gekennzeichnet, dass mehrere Konfigurationswerte eingesetzt werden, und je Betriebsart ein eigener Konfigurationswert verwendet wird und/oder pro Betriebsart verschiedene Konfigurationswerte unterschieden werden.

6. Vorrichtung zur Steuerung von Betriebsabläufen insbesondere beim Fahrzeug, mit einer Funktionseinheit, insbesondere einer Steuereinheit, welche eine Verbindung zu einem Bussystem aufweist, sowie einer Überwachungseinheit, welche die Funktionseinheit und/oder das Bussystem überwacht, wobei die Überwachungseinheit die Verbindung der Steuereinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff trennt, dadurch gekennzeichnet, dass die Vorrichtung weiterhin Mittel enthält, durch welche die Funktionseinheit den Zugriff der Überwachungseinheit konfiguriert.

7. Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere bei einem Fahrzeug, welche mit einer Funktionseinheit, insbesondere einer Steuereinheit in Verbindung steht, wobei die Vorrichtung eine Verbindung zu einem Bussystem aufweist, wobei die Vorrichtung eine Überwachungseinheit enthält, welche die Funktionseinheit und/das Bussystem überwacht, wobei die Überwachungseinheit die Verbindung der Funktionseinheit mit dem Bussystem in einem Sicherheitsfall durch Zugriff trennt, dadurch gekennzeichnet, dass die Vorrichtung weiterhin Mittel enthält, durch welche die Funktionseinheit den Zugriff der Überwachungseinheit konfiguriert.

8. Vorrichtung nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass die Mittel als Konfigurationsmittel einen Speicherbereich umfassen, in welchem wenigstens ein Konfigurationswert speicherbar ist und der Zugriff abhängig von den Konfigurationswert konfiguriert wird.

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass die Verbindung der Funktionseinheit zum Bussystem mit einer Verbindungseinheit, insbesondere einer Treiberschaltung, realisiert ist und dass die Überwachungseinheit und/oder die Mittel, insbesondere der Speicherbereich, und/oder die Verbindungseinheit in einer Schaltungseinheit integriert sind.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 30 996 A1
Int. Cl.[7]: G 05 B 9/02
Offenlegungstag: 10. Januar 2002

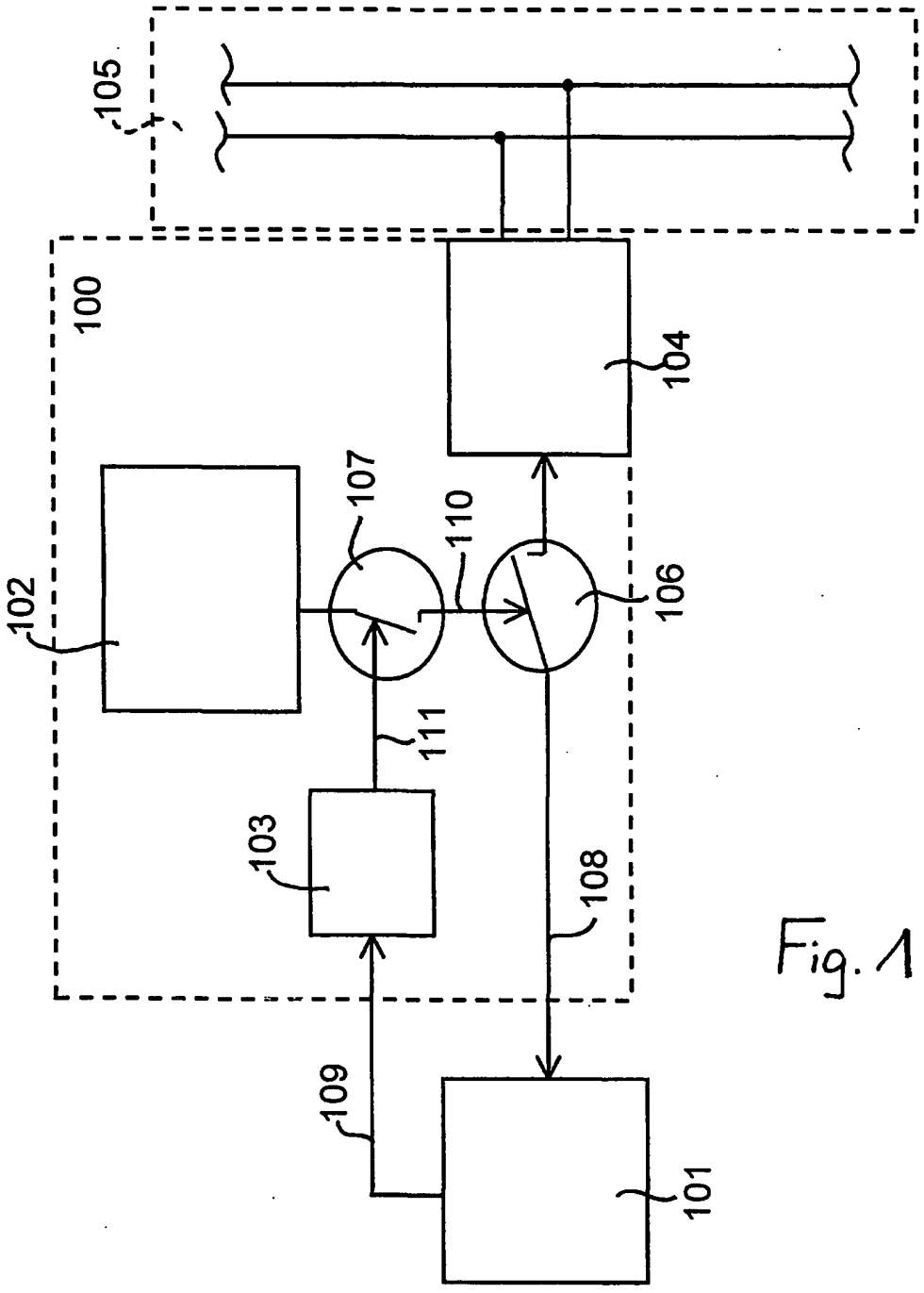


Fig. 1

Nummer: DE 100 30 996 A1
Int. Cl.[7]: G 05 B 9/02
Offenlegungstag: 10. Januar 2002

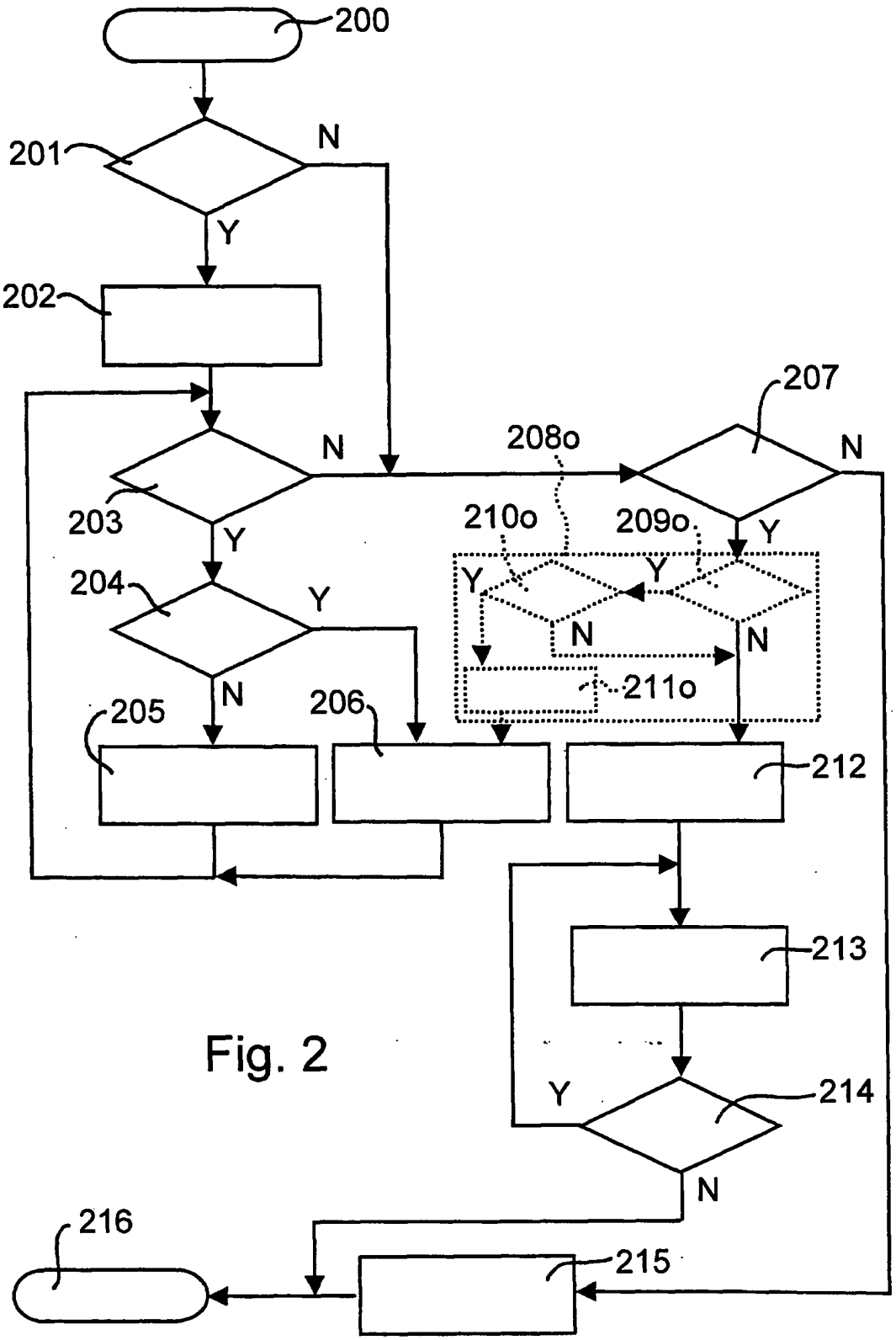


Fig. 2